REMARKS

This Amendment is responsive to the Office Action dated June 7, 2003. All rejections and objections of the Examiner are respectfully traversed. Reconsideration is respectfully requested.

At paragraphs 1 and 2 of the Office Action, the Examiner rejected claims 8-9 for indefiniteness under 35 U.S.C. 112, second paragraph. Amendments to the claims are believed to satisfy all requirements of the Examiner in this regard.

At paragraphs 3 through 11, the Examiner rejected claims 1-5, 8-11, and 13-17 as being obvious under 35 U.S.C. 103, citing an article in the publication "Network Computing" by Gregory Yerxa ("Yerxa"), in combination with an article in the publication "PC/Computing" by Ed Bott ("Bott"). Applicants respectfully traverse this rejection.

Yerxa is an article generally describing security improvements made in the Java software system. As described by Yerxa, the Java Virtual Machine (JVM) includes a Class Loader (CL), a Byte-Code Verifier (BCV), and a Security Manager. Yerxa discloses that the Java Security Manager (SM) is a Java class, and controls the performance of potentially dangerous activities. Yerxa states that the SM monitors file access, system I/O, network I/O, Class Loader instantiation, process/thread creation and access to Java class objects. As described by Yerxa, when an applet performs one of the actions monitored by the SM, the applet first consults the SM for approval. The SM decides if the action is permissible based on the origin of the application or applet. Whenever a potentially dangerous function is called from within the applet or application, the SM grants or denies access to specific resources based on the origin of the application or applet.

Yerxa also discloses that the Java system restricts *access to* applets and applications based on their origins. Applets that are embedded in Web pages are most restricted, while local Java applications are trusted almost entirely without restrictions. Users may grant more access to certain applets, and this is enabled by denoting specific applets as trusted, thus overriding the normal default setting that all applets are untrusted and cannot access local information. Yerxa further teaches that an administrator can allow or deny specific access to the network based on an applet's origin.

The Bott article covers issues of security with regard to the Internet, and predates the Yerxa article. Bott discloses that Java and JavaScript are very dangerous, and advises users to disable them there machines to improve security. Bott also generally describes public key encryption, digital signatures, and digital certificates.

Nowhere in the combination of Yerxa and Bott is there disclosed or suggested any system or method for providing security against unauthorized access to internal resources of a network device that includes receiving a digital signature, requesting a de-encryption code, de-encrypting the digital signature with the de-encryption code, authenticating the de-encrypted digital signature and, responsive to the authenticating of the de-encrypted digital signature, ***obtaining an access level for program code associated with the digital signature, and, responsive to the obtained access level, requesting allowed operations associated with the access level with respect to the program code, responsive to processing of the program code,*** as in the present independent claims 1, 8 and 13.

The combination of Yerxa and Botts teaches using digital signatures to control *access to* applets associated with the digital signatures, and for purposes of determining the validity of the applets. Yerxa and Botts include no hint or suggestion of using a de-encrypted digital signature to obtain an access level for a portion of program code to be used while processing the program code, as in the present independent claims 1, 8 and 13. In contrast, Yerxa teaches that the origin of an applet may be determined by where it is executed from. Specifically, Yerxa provides an example in which a user downloads an applet from within a local Web browser, and then executes it locally, outside the browser. In this case, Yerxa teaches that the origin of the applet is considered to be local, within the local executing machine, and accordingly the JVM allows access to local information because such a local origin makes the executing applet trusted. If the user viewed the applet from within the Web browser, the system described in Yerxa would permit the applet less access to the local system, simply because the applet was executed from within the context of the browser.

With regard to digital signatures, Yerxa discloses that digital signatures can be used to verify content during a download, and that an administrator can restrict access to an applet based on its associated digital signatures or author information. Yerxa also notes that digital signatures are particularly effective in identifying valid applets because signatures are quickly recognized and may be stored for future access. Similarly, and as noted above, Botts teaches that digital signatures are useful for validation purposes, but includes nothing suggesting the possibility of using the contents of a digital signature to obtain access level information to be used to control access to system resources while processing a portion of program code, as in the present independent claims 1, 8 and 13. Moreover, Yerxa teaches away from the use of digital signatures in the determination of the source of program code, indicating that some uses of digital signatures to identify the origin of an applet, based on public knowledge of Java byte code, may be misleading and result in a security risk.

For the above reasons, Applicants respectfully urge that the combination of Yerxa and Bott does not disclose all the features of the present independent claims 1, 8 and 13. Accordingly, the combination of Yerxa and Bott does not form the basis for a *prima facie* case of obviousness under 35 U.S.C. 103 with regard to claims 1, 8 and 13. As to claims 2-5, 9-11 and 14-17, they each depend either directly or indirectly from claims 1, 8 or 13, and are believed to be patentable over the combination of Yerxa and Bott for at least the same reasons. Reconsideration of claims 1-5, 8-11, and 13-17 is respectfully requested.

At paragraph 12 of the Office Action, the Examiner indicated that dependent claims 6-7, 12 and 18 contained allowable subject matter. Claims 6, 12 and 18 have accordingly been re-written in independent form, and are now believed to be allowable.

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone the undersigned Attorney at 978-264-6664 so that such issues may be resolved as expeditiously as possible.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

October 7, 2003
Date

David A. Dagg
David A. Dagg, Reg. No. 37,809
Attorney/Agent for Applicant(s)
Steubing McGuinness & Manaras LLP
125 Nagog Park Drive
Acton, MA 01720
(978) 264-6664

Docket No. 120-300
Dd: 10/07/2003